DATE(S) ISSUED:
09/04/2020

SUBJECT:
A Vulnerability in WordPress File Manager Plugin Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the File Manager plugin that could allow for remote code execution. WordPress is a web-based publishing application implemented in PHP, and the File Manager Plugin allows site Admins to upload, edit, delete files and folders directly from the WordPress backend without having to use FTP. Successful exploitation of this vulnerability could allow for remote code execution in the context of the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Application accounts that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:
On August 25th, A proof of concept (PoC) exploit script was published to a Github repository. In addition, there are reports of these of this vulnerability being actively exploited in the wild.

SYSTEM AFFECTED:

- File Manager versions 6.0 – 6.8

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in the File Manager plugin that could allow for remote code execution. This vulnerability exists due to the improper inclusion of an open-source file manager library called elFinder. It appears that the file “connector.minimal.php-dist” was stored in an

executable format (renamed to .php) and the file “could be accessed by anyone”. An attacker could exploit this flaw by sending a specially crafted request to the connector.minimal.php file which can lead to remote code execution in the context of the application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Application accounts that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by File Manager to affected systems, immediately after appropriate testing.
- Apply the Principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:

Wordfence

https://www.wordfence.com/blog/2020/09/700000-wordpress-users-affected-by-zero-day-vulnerability-in-file-manager-plugin/

Github

https://github.com/w4fz5uck5/wp-file-manager-0day